

## The Information Agenda

Paul Wilson

Director of Government Relations, De La Rue

### **Information Governance: The Core Issues**

The core issues of Information Governance are well appreciated and the subject of regular media coverage, but are rarely brought together to show the extent of the issue. For the sake of clarity in this document they are:

#### Security

- Privacy of Personal Data
- Confidentiality of Sensitive Public Sector Information (EG Classified Material)
- Good custody of Personal and Public sector information by private sector entities

#### Access

- Public access to Government Information
- Disclosure of Corporate information
- Sharing of information across government departments or indeed between governments

**Other areas such as the unauthorised disclosure of private sector sensitive information (EG insider trading) have not attracted the same degree of interest in the broader media beyond the financial pages.**

**The Private sector's operational interest in the core issues is driven not by concerns for the civil issues of privacy or freedom of information, but by operational expedients along the lines of : ' how little do I have to keep in order to comply with legal requirements of disclosure in the event of legal proceedings.'**

**The six 'core issues' broadly apply to three information 'sectors':**

## **1. Personal data.**

Covered by Data Protection legislation, but a source of constant concern, partly because of the Civil Liberties/privacy question, partly because of the increasing incidence of Identity Fraud and Identity Theft therefore of widest concern, because it impacts each and everyone of us. Most recent losses of service personnel details might be seen as straddling the first three core issues.

## **2. Public Sector/Government information.**

Control (IE retention or disclosure) of Government information is in some instances strictly prescribed by operational procedures such as document classifications and legislation setting out limitations on release to the public. To redress the balance of accessibility against security, Freedom of Information legislation attempts to give limited access to public sector information on request which would not be disclosed as a matter of course.

The term 'Public' will be used as shorthand for this sector, even though it is as inelegant as the word 'Public' in an educational context.

## **3. Private Sector (commercial) information.**

Apart from information which is sensitive to the commercial operations of the private entity involved, private sector information will often be relevant to the first category ( Personal Information ) EG : banking details; and in some specialist cases, will be relevant to the Second category ( Public sector information ). EG in the area of defence procurement.

Sensitive information held by the voluntary sector and by other entities which do not comfortably fit into the three categories listed above are most likely to be relevant to the first core issue ( privacy) and to be controlled (IE retained or disclosed) on the basis of conventions or working practices specific to the entity or the profession. This would, for instance, include professional codes of conduct relating to the medical and legal professions which long pre-date legislation in the privacy area.

Core issues will often intersect the various Information sectors creating an interlocking set of considerations in compiling a

coherent and comprehensive Information Retention and Disclosure policy.

Some Examples are :

Issues	Privacy	Public Sector	Private Sector
Personal		Health	Banking
Classified	Service Personnel	Defence	Defence Contracting
Custody ( private sector for Public sector)	Driving Licence data	Defence contracting	
Public access		Transparent Government	Arbitration.
Corporate Disclosure	Arbitration. Personal claims	Contract Tendering	Legal Challenges
Shared (across government)	Advanced Passenger Information	Terrorist investigation	Fraud

## **Data Lost**

Recent scandals have touched on all of these categories: The loss of sensitive cabinet office documents on al –Qaeda on a commuter train plainly indicated a lapse of procedure on the part of a public sector official in a government department which handles the most sensitive information on a daily basis.

The loss of two discs from HMRC containing banking details on no fewer than 25 million individuals is attributable to a failure in common sense at a government department, rather than a failure in adhering to standard operating procedure. Ironically, it was a failure as a result of corner –cutting to achieve a relatively paltry financial saving.

Personal data on RAF personnel were stolen from RAF Innsworth, the Headquarters of the RAF's personnel branch and, it would be assumed, a highly secure and well protected site. The stories could hardly get worse.

However , as if to prove that lapses in proper handling of sensitive information are not the sole prerogative of the Civil Service , personal data on the UK's prison population was lost when an apparently opportunist thief stole a memory stick from the offices of a private sector consulting company working on a Home Office Contract.

And, in a world where Public sector operations are increasingly outsourced to private sector companies possibly headquartered overseas, we see – and will continue to see – lapses in data security by private sector entities abroad with negative consequences for government and the individual. A further telling example of this is the loss in the US of data relating to 3 Million learner drivers on a disc held by a company working with the UK's Driving Standards Agency.

It had been thought that these were the most recent examples of leaks in the national data plumbing. However, even as this paper was being concluded, reports of the loss of an un-encrypted hard

drive containing personal data relating to 100,000 - 200,000 service personnel have appeared in the media.

But, in terms of volume, the greatest single source of loss or disposal of data on individuals is probably attributable to the individuals themselves. Despite regularly repeated advice on destruction of papers bearing sensitive personal information, UK citizens dispose of significant volumes of documents which are of material use to criminals in pursuit of identity fraud or identity theft. This, however, is no comfort to Public and Private sector companies which are held by the public to have a duty to guard sensitive data – of either a personal or public nature – with the utmost care.

But, what the private citizen does with his or her personal data, remains, by and large, his or her own affair.

The public, therefore the media and, consequently, legislators are highly sensitised to the issues

## **What frames Information Retention and Disclosure Policies?**

### **Data Retained**

An internet survey of some of the available material on Information retention or Document retention policies makes it clear that, alongside Data Protection Act compliance, the single most important factor in shaping corporate policy is the need to preserve documents against the possibility of legal proceedings or to address some other issue of governance: a follow-up inquiry on a tax return ;the possibility of a staff grievance or arbitration procedure. In particular, the statutory limitations applicable to a range of such proceedings will determine the length of time that documents are preserved.

It is also clear that different legal regimes have different statutory limitations for different aspects of the law: land as opposed to tax and so on.

***The parameters for information retention are set by legislation and particularly by statutory limitations.***

***It is difficult to see how Business can bring sense to the onward march of complex legislation, much less steer it without a coordinated campaign to influence primary legislation across a wide range of subjects.***

***Business will always be obliged to respond to legislation wherever it touches on document retention, rather than set out to influence policy 'upstream' purely for the sake of a more sensible document retention regime, simply because most businesses are already overstretched in their daily operations and where they lobby actively, this is in pursuit of very specific operational or indeed contractual requirements. Lobbying in pursuit of a more rational, cohesive and simplified document retention and disclosure policy in the UK would be beyond the resource of individual UK companies and could only sensibly be pursued on their behalf by Trade associations working in collaboration with Industry bodies such as the CBI.***

## **Data Disclosed**

As statutory limitations differ significantly from country to country (See Global Counsel: October 2003: *Document retention around the world*), companies subject to a range of legal systems due to their having operations in many different countries around the world may have to play safe by preserving documents and data for the longest period demanded by any one of the relevant jurisdictions.

For example, US courts can demand disclosure of information, held, say, in Europe. Should, therefore, European businesses retain documents in line with US statutory limitations? (See COULTAL's white paper: *Impact of International regulations on Electronic Document Retention and Destruction* particularly for the Intel case.) And if US statutory limitations set the benchmark, why not that of other countries?

***UK policymakers can and should attempt to bring some sense to a situation where corporate information retention and disclosure policies of foreign jurisdictions muddy the waters for UK businesses.***

*Again, individual businesses could not and would not want to spend their time lobbying government piecemeal on this issue. Only an industry body such as the CBI could bring powers of coordination and broad industry perspectives to bear on the issue.*

## **Data Shared**

The sharing of information across Government Departments and between governments forms one of the most contentious aspects of Information Governance for many.

For example, the present Government's plan to link up various existing departmental data bases into a National Identity register has been strongly contested by the Conservative party which has repeatedly stated its intention of dismantling or at least, 'disaggregating', such a register.

Single interest lobby groups such as No2ID similarly present consistent and vocal opposition to the Identity register plan.

However, it is clear that there already exists some degree of data sharing across government departments at an operational level. An obvious instance of this is the ability of the Police to check driving licence information with the DVLA.

Indeed, failures to share information (as in the Soham murder case) are possibly perceived by the media and the public as a greater failure than some of the data leaks mentioned above.

Plainly a degree of data sharing between government departments is not only unavoidable, but is already a fact and is indeed desirable.

However, persistent failures in confidential data management by both officials and private sector operations have undermined the credibility of a National Identity register before it has been established. Under what circumstances would data on an individual's health, say, be passed to other government departments? Will commercialisation of the National Identity Register operation lead to an individual's personal details being revealed to private sector operations?

Information sharing between governments, similarly, already exists on classified matters subject to very tight procedures.

But it is when the inter-governmental data sharing begins to impinge on personal liberties or personal data, that the data sharing becomes suspect in the eyes of the public. Advanced passenger profiling and the possibility of, for instance, onward release of data in an EU investigation in to criminal activities via the Schengen Information System to non EU organisations (EG the possibility of information being passed by Europol to the American Courts) are both cases in point.

*As far as business is concerned, the proliferation of information sharing between governments is something best left to governments. At best intergovernmental information exchange is a business opportunity; at worst a further inconvenience. It is not likely to be a major reason for transferring a company from one jurisdiction to another – unless, that is, the company concerned has something to hide.*

### **A data –handling Culture**

In some areas of the Government machine – particularly in highly sensitive areas such as Defence and Foreign Policy – there is a strict classification of documentation which governs the way in which it is held and treated. By and large (notwithstanding the occasional breach) the system works. It is well oiled and adherence to the system is a standard operating procedure which people more often than not have come to accept as second nature. Failure to comply with the standard operating procedures surrounding the handling of sensitive documents in this type of Government Department is sanctioned.

In contrast, there is another type of Government Department which, traditionally, has never handled particularly sensitive documentation. The loss of policy documentation, say , from the Department of Culture Media and Sport , is more likely to lead to embarrassment than to a threat to national security. For this reason, those departments have no ingrained culture of Document Security, no standard operating procedure in the handling of data and information. As long as those departments are not handling significant volumes of personal data, it seems unlikely that there

will be a data loss scandal. However, in the event of any major exchange of information between the Cabinet office and DCMS on security threats to the 2012 Olympics, even this department which is relatively inexperienced in handling sensitive information will be vulnerable to the possibility of embarrassing information loss. And, just as public and media sensitivity to the issue rises with every new leak or loss, an increasing number of government departments and private sector entities will be forced to drive up their information handling standards. The problem has the potential to ripple out to areas of government or industry which are not familiar with the best practices of a data handling culture.

***The more information we share, the more likely, in the present circumstances, we are to experience serious losses.***

### **Where does best practice currently sit?**

Few Private sector entities have a classified data handling culture as solid as that of, for instance, GCHQ, which probably remains the gold standard for managing high volumes of sensitive data.

The recent losses of data by private sector consultancy and IT companies supports the argument that the private sector is weak in this area, although the List X regime (the management of which has been re-allocated from the Security Service to Ministry of Defence in recent years) has given some defence contractors a solid procedural base for operating in an environment which requires tight control of classified information.

***There are indications that List X operating standards are being applied to other governmental operations outside the narrow defence arena. However, in the long term, a civil equivalent – a set of standard operating procedures – should be developed as the norm for all government departments and private sector contractors handling information which clearly falls into the sensitive category.***

***The Private sector should be involved in drawing up these operating procedures, but ultimate responsibility for standards must rest with officials and politicians. If commercial entities alone are left to set the standards, it is unlikely that public confidence – and accountability of institutional stakeholders – will be achieved to any credible extent. The public can reasonably***

*expect Officials, Politicians and the private sector to work together to resolve these issues.*

### **Standard Operating Procedures.**

The suggestion of a set of operating procedures is beyond the remit of this paper. However, one glaring and unavoidable fact points in a particular direction. In an overwhelming number of cases, loss of information has occurred as result of data being downloaded onto memory sticks or discs (including hard discs on PCs) and then removed from a secure site. In other instances (according to the most recent MOD revelation), not content with losing the memory stick or disc, the temporary custodian of the data has lost the entire PC. It would seem that technology, far from tightening up information governance has made it much easier.

*A much tighter regime , including ,for instance , forbidding the use of memory sticks or removable discs for certain types of information in specific restricted areas must be one of the measures for consideration.*

*Similarly, it is time to consider whether individuals – either official of contractors – should be allowed to take PCs containing sensitive information out of controlled environments – even if this results in inconvenience ( and perhaps revised expectations in productivity.)*

*Experiences so far show that technology has, if anything, contributed to the ease with which data is lost and we must therefore conclude that there is no substitute for tight operating procedures as the main means of heading off the human predilection for cock-up.*

### **TIME FOR ANOTHER REVIEW?**

No. Especially as it would seem that recommendations of the Poynter review were not followed through.

*The Government now needs to move forward as a matter of urgency to the preparation of standard operating procedures for handling personal and public sector data managed by the Government.*

*The Government should also commission a body such as the CBI to work with a wide range of businesses in putting together recommendations for information handling – both retention and disclosure. Whilst these recommendations will be drawn up by industry, it makes sense for officials to be part of the process – replacing for the duration of this exercise, what has become the standard practice of drawing private sector expertise into government, with a secondment, instead, of officials from Whitehall into industry.*

*The industry recommendations, once agreed at the appropriate levels in Whitehall and Westminster should act as the basis for cohesive and comprehensive guidance to industry on best practice. The idea that further legislation will improve the situation must remain open to doubt. Standard operating procedures for Government departments and contractors and a code of best practice across industry are long overdue.*

Paul Wilson

De La Rue

*The views expressed in this paper are those of the author and not necessarily those of De La Rue.*